PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-275115
(43)Date of publication of application : 13.10.1998

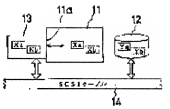
(51)Int.Cl. G06F 12/14
G09C 1/00
H04L 9/10

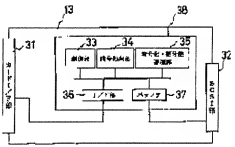
(21)Application number : 09-080241
(22)Date of filing : 31.03.1997

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : KAWAKUBO HIDEJI
TAKADA SHUNSUKE
YAMANAKA KIYOSHI

(54) DATA CIPHERING AND STORING METHOD AND SYSTEM DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide the data ciphering and storing method and system device which can prudentially manage ciphered data stored in an external storage device by using a computer card.
SOLUTION: Under the control of a control part 33, plaintext data Xa and Xb are ciphered sequentially by using a ciphering key Ka stored in a ciphering and deciphering key storage part 35 to generate corresponding ciphered data Ya and Yb in a process of transfer of the plaintext Xa and Xb expanded in the main storage device of an information terminal device to the external storage device 12. In a process of transfer of ciphered data Ya and Yb written temporarily in the external storage device 12 to the information processor 11, the ciphered data Ya and Yb are deciphered sequentially by using a deciphering key Kb stored in the ciphering and deciphering key storage part 35 to restore the original plaintext data Xa and Xb by a ciphering process part 34, which is constituted in a small-sized, lightweight computer card 13 having an authenticating function of the user individual.





CLAIMS

[Claim(s)]
[Claim 1]On the occasion of preservation of plaintext data developed by main memory unit of information terminal equipment, according to predetermined configuration, set a preservation destination of the plaintext data concerned as an external storage, and this is changed into an accessible state, When saving said plaintext data at an external storage which it changed into the accessible state concerned, In a process in which the plaintext data is transmitted to said external storage, encryption processing is sequentially performed to the plaintext data concerned using an enciphering key which uses a predetermined cryptographic algorithm and its data encryption function, While writing encryption data generated by this encryption processing corresponding to said plaintext data in said external storage, When reading said encryption data once written in an external storage which it changed into the accessible state concerned, In a process in which the encryption data is transmitted to said information terminal equipment, decoding processing is sequentially performed to the encryption data concerned using a decode key which uses said predetermined cryptographic algorithm and its data decryption function, A data encryption preserving method characterized by what plaintext data of origin restored by this decoding processing is developed for to a main memory unit of said information terminal equipment.
[Claim 2]It replaces with said decode key which uses said enciphering key and a data decryption function to use a data encryption function of said predetermined cryptographic algorithm, The data encryption preserving method according to claim 1 characterized by what encryption processing of said plaintext data and decoding processing of said encryption data are performed for using a single common key which uses each function both.
[Claim 3]When writing said encryption data in said external storage, and when reading said encryption data from said external storage, The data encryption preserving method according to claim 1 or 2 characterized by what necessary interface converting according to interface form of said external storage is performed for to the encryption data concerned.
[Claim 4]The data encryption preserving method according to claim 3 characterized by what said predetermined interface converting is performed for according to the SCSI form concerned as said external storage using what adopted SCSI form.
[Claim 5]Information terminal equipment possessing a card slot.
An external storage in which access by this information terminal equipment is possible.
A possible computer card of using it, equipping a card slot of said information terminal equipment, and it being used for it, carrying out cable connection to said external storage, and performing data transfer mutually between a main memory unit of the information terminal equipment concerned, and said external storage.
A right-to-access setting-out means for it to have, and for it to be constituted, and for said computer card concerned to set up the right to access to said external storage, and to make said information terminal equipment recognize this.
A data encryption function and a data decryption function.
When saving plaintext data which is the data encryption preservation system unit provided with the above, and was developed by main memory unit of said information terminal equipment at said external storage, the plaintext data in a process transmitted to said external storage. Encryption processing is sequentially performed to the plaintext data concerned, using said cryptographic algorithm memorized by said cryptographic algorithm memory measure and said enciphering key accumulated in said key accumulation means, In the state where the right to access concerned was set up by encryption processing means to create encryption data corresponding to said plaintext data, and said right-to-access setting-out means. When reading said encryption data once written in said external storage, the encryption data in a process

transmitted to said information terminal equipment. Decoding processing is sequentially performed to the encryption data concerned, using said cryptographic algorithm memorized by said cryptographic algorithm memory measure and said decode key accumulated in said key accumulation means, and it has a decode processing means which restores the original plaintext data.

[Claim 6]Said key accumulation means is what accumulates a single common key which uses both data encryption functions and data decryption functions of said cryptographic algorithm that were memorized by said cryptographic algorithm memory measure, The data encryption preservation system unit according to claim 5 characterized by what said encryption processing means and said decode processing means are what performs encryption processing of said plaintext data and decoding processing of said encryption data using said common key accumulated in the key accumulation means concerned, respectively.
[Claim 7]The data encryption preservation system unit according to claim 5 or 6 characterized by what functional constitution of said cryptographic algorithm memory measure which constitutes said computer card, said key accumulation means, said encryption processing means, and said decode processing means is carried out by one chip element, and is changed.
[Claim 8]The data encryption preservation system unit according to claim 5, 6, or 7 characterized by what is been a thing which said right-to-access setting-out means sets [thing] up the right to access concerned automatically by wearing of said computer card to a card slot of said information terminal equipment, and makes said information terminal equipment recognize this.
[Claim 9]When writing said encryption data in said external storage by said encryption processing means, And when reading said encryption data from said external storage by said decode processing means, The data encryption preservation system unit according to claim 5, 6, 7, or 8 characterized by what it has further an interface converting means to perform necessary interface converting according to interface form of said external storage for.
[Claim 10]The data encryption preservation system unit according to claim 9 which SCSI form is used for said external storage, and is characterized by what said interface converting means is what performs said necessary interface converting according to the SCSI form concerned.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention about a data encryption preserving method and a system unit in detail, When saving the plaintext data created in information terminal equipment, such as a personal computer, at external storages, such as a hard disk drive, When developing the encryption data which enciphered plaintext data in the process of the transmission, and was saved by this at the external storage to the main memory unit of information terminal equipment, It is involved in the data encryption preserving method which decoded encryption data in the process of the transmission, and the data encryption preservation system unit directly used for the operation.
[0002]
[Description of the Prior Art]When it is going to encipher and save the plaintext data which generally comprises the document etc. which were drawn up in information terminal equipment, such as a personal computer, for the security, in the former. Based on processing of the application software for document preparation, the plaintext data after creation in the state where the main memory unit developed, It once saves and (namely, usual processing at the time of closing a document) ranks second to data files, such as an internal hard disk, with a gestalt as it is, It is made to perform processing for necessary encryption to the plaintext data in the state where it was saved at the data file concerned based on processing of the application software for cipher processing.
[0003]In enciphering and saving plaintext data first as shown in drawing 4 if it explains briefly per processing of the application software for the cipher processing, The data once saved at the data file 1 is read (ST1), The data form is checked (ST2), when it is plaintext data (plaintext data which is trying to encipher), processing for necessary encryption is performed (ST3) and the encryption data obtained by this is written in the data file 1 (ST4).
[0004]In order to use again the encryption data once saved by the above processing at the data file 1 on the application software for document preparation, Since it is necessary to save again at the data file 1 and to develop this to the main memory unit of information terminal equipment further after reading this from the data file 1 and decoding it, When the data form checked in processing of above-mentioned ST2 is encryption data (encryption data which is trying to decode), After performing processing for necessary decoding in processing of ST3, the plaintext data obtained by this is written in the data file 1 in processing of ST4.
[0005]
[Problem(s) to be Solved by the Invention]As mentioned above, if it is in encryption processing of the conventional plaintext data, Based on processing of the application software for document preparation, the plaintext data concerned developed by the main memory unit of information terminal equipment, Certainly it once saves at the data file 1, a result which requires time suitable in order to perform the necessary encryption processing since to perform encryption processing anew is needed is brought after that, and the good thing can never say operativity for the user of the system concerned.
[0006]The encryption data obtained by encryption processing, It is saved uniformly for the data file 1 in information terminal equipment, and management of the right to access, Usually, since it is performed by the attribute flag of the data management part in an information-terminal-equipment device, those who do not have the right to access essentially can also change the right to access concerned easily only by rewriting of this attribute flag. For this reason, when an unauthorized use is tried for example, by the person expert in the composition of this kind of system, there is a danger of the theft of the encryption data saved by that unauthorized use person at the data file 1 being carried out, or being eliminated.
[0007]Set the preservation destination of this point, for example, encryption data, as external storages,

such as an outer hard disk device, and at the time of intact of a system. The external storage should be removed and the theft of the encryption data by an above-mentioned unauthorized use person and the danger of elimination should always become [make / this / in the bottom of a regular user's management] small by leaps and bounds.
[0008]However, it is very difficult for making an external storage also under an always regular user's management actually. The one most effective for performing this is not practical, considering the size or weight, although it is that a user always carries an external storage at the time of intact of a system.
[0009]When actually managing encryption data with an external storage, to use with no converting, without making a change of the hardware is desired. Since SCSI form (SCSI: Small Computer System Interface) is being especially standardized as a form of the interface to information terminal equipment in the field of an external storage, If it can do, I would like to apply this interface form as it is.
[0010]In here, the main purposes that this invention should be solved are as follows. That is, the 1st purpose of this invention is to provide the possible data encryption preserving method and system unit of performing necessary encryption processing to the inside of a short time efficiently.
[0011]The 2nd purpose of this invention is to provide the data encryption preserving method and system unit which eliminated danger by an unauthorized use person, such as a theft of encryption data, and elimination, by managing necessary encryption data with an external storage.
[0012]The 3rd purpose of this invention is to provide the possible data encryption preserving method and system unit of managing perfectly the encryption data saved at the external storage, without always carrying an external storage.
[0013]The 4th purpose of this invention is to provide the data encryption preserving method and system unit of SCSI form in which application to an external storage is possible.
[0014]Other purposes of this invention will become naturally clear from the statement of each claim of a specification, a drawing, especially a claim.
[0015]
[Means for Solving the Problem]This invention constitutes a function which creates encryption data from plaintext data developed by main memory unit of information terminal equipment in solution of an aforementioned problem in a computer card (what is called a PC card) which has a user individual's authentication function, This computer card is made to intervene between information terminal equipment and an external storage, and is used, and it restricts to the time when information terminal equipment was equipped with that computer card, further, and has the feature of granting the right to access of an external storage to information terminal equipment.
[0016]If it states to a concrete detail, when this invention adopts each new characteristic configuration method and means of next enumerating, by solution of the technical problem concerned, it will be accomplished so that said purpose may be attained.
[0017]Namely, preservation of plaintext data developed by main memory unit of information terminal equipment is faced the 1st feature of this invention method, According to predetermined configuration, set a preservation destination of the plaintext data concerned as an external storage, and this is changed into an accessible state, When saving plaintext data at an external storage which it changed into the accessible state concerned, In a process in which the plaintext data is transmitted to an external storage, encryption processing is sequentially performed to the plaintext data concerned using an enciphering key which uses a predetermined cryptographic algorithm and its data encryption function, While writing encryption data generated by this encryption processing corresponding to plaintext data in an external storage, When reading encryption data once written in an external storage which it changed into the accessible state concerned, In a process in which the encryption data is transmitted to information terminal equipment, decoding processing is sequentially performed to the encryption data concerned using a decode key which uses a predetermined cryptographic algorithm and its data decryption function, It is in composition adoption of a data encryption preserving method which develops plaintext data of origin restored by this decoding processing to a main memory unit of information terminal equipment.
[0018]The 2nd feature of this invention method is replaced with a decode key which uses an enciphering key and a data decryption function to use a data encryption function of a predetermined cryptographic algorithm in the 1st feature of an above-mentioned this invention method, It is in composition adoption of a data encryption preserving method which performs encryption processing of plaintext data and decoding processing of encryption data using a single common key which uses each function both.
[0019]When the 3rd feature of this invention method writes encryption data in the 1st or 2nd feature of an above-mentioned this invention method in an external storage, And when reading encryption data from an external storage, it is in composition adoption of a data encryption preserving method which performs

necessary interface converting according to interface form of an external storage to the encryption data concerned.

[0020]The 4th feature of this invention method is in composition adoption of a data encryption preserving method which performs predetermined interface converting in the feature according to the SCSI form concerned using what adopted SCSI form without considering it as an external storage in the 3rd feature of an above-mentioned this invention method.

[0021]Information terminal equipment with which the 1st feature of this invention device possesses a card slot on the other hand, Use it, equipping a card slot of an external storage in which access by this information terminal equipment is possible, and information terminal equipment, and it is used for it, carrying out cable connection to an external storage, Between a main memory unit of the information terminal equipment concerned, and an external storage, have a possible computer card of performing data transfer mutually, and it is constituted, A right-to-access setting-out means by which the computer card concerned sets up the right to access to an external storage, and makes information terminal equipment recognize this, A cryptographic algorithm memory measure which memorizes a cryptographic algorithm provided with a data encryption function and a data decryption function, An enciphering key which uses a data encryption function of a cryptographic algorithm memorized by this cryptographic algorithm memory measure, When saving plaintext data developed by main memory unit of information terminal equipment at an external storage in the state where the right to access concerned was set up by key accumulation means which accumulates a decode key which uses a data decryption function, and a right-to-access setting-out means, the plaintext data in a process transmitted to an external storage, Encryption processing is sequentially performed to the plaintext data concerned, using a cryptographic algorithm memorized by cryptographic algorithm memory measure and an enciphering key accumulated in a key accumulation means, In the state where the right to access concerned was set up by encryption processing means to create encryption data corresponding to plaintext data, and a right-to-access setting-out means, When reading encryption data once written in an external storage, the encryption data in a process transmitted to information terminal equipment, Using a cryptographic algorithm memorized by cryptographic algorithm memory measure and a decode key accumulated in a key accumulation means, decoding processing is sequentially performed to the encryption data concerned, and it is in composition adoption of a data encryption preservation system unit which has a decode processing means which restores the original plaintext data.

[0022]A key accumulation means in the 1st feature of the above-mentioned this invention device the 2nd feature of this invention device, It is what accumulates a single common key which uses both data encryption functions and data decryption functions of a cryptographic algorithm that were memorized by cryptographic algorithm memory measure, An encryption processing means and a decode processing means in the feature are in composition adoption of a data encryption preservation system unit which is what performs encryption processing of plaintext data and decoding processing of encryption data, respectively using a common key accumulated in the key accumulation means concerned.

[0023]A cryptographic algorithm memory measure which constitutes a computer card [in / in the 3rd feature of this invention device / the 1st or 2nd feature of the above-mentioned this invention device], A key accumulation means, an encryption processing means, and a decode processing means are in composition adoption of a data encryption preservation system unit in which functional constitution is carried out by one chip element and which changes.

[0024]A right-to-access setting-out means in the 1st, 2nd, or 3rd feature of the above-mentioned this invention device the 4th feature of this invention device, The right to access concerned is automatically set up by wearing of a computer card to a card slot of information terminal equipment, and it is in composition adoption of a data encryption preservation system unit which is a thing which makes information terminal equipment recognize this.

[0025]When the 5th feature of this invention device writes encryption data in an external storage by an encryption processing means in the 1st, 2nd, 3rd, or 4th feature of the above-mentioned this invention device, And when reading encryption data from an external storage by a decode processing means, it is in composition adoption of a data encryption preservation system unit which has further an interface converting means to perform necessary interface converting according to interface form of an external storage.

[0026]An external storage in the 5th feature of the above-mentioned this invention device the 6th feature of this invention device, SCSI form is adopted and an interface converting means in the feature is in composition adoption of a data encryption preservation system unit which is what performs necessary interface converting according to the SCSI form concerned.

[0027]
[Embodiment of the Invention]Hereafter, an embodiment of the invention is described per the example of a device, and example of a method, referring to an accompanying drawing.
[0028](Example of a device) First the composition of the data encryption preservation system unit concerning this embodiment, The information terminal equipment 11 which comprises a personal computer etc. as basic constitution of a system as shown in drawing 1, It has the external storage 12 which comprises the outer hard disk device (a usual magnetic disk drive and optical-magnetic disc equipment) etc. of the SCSI form in which access by this information terminal equipment 11 is possible. And the computer card 13 which the main formation parts of this invention are accomplished and can perform data transfer mutually between the main memory unit of the information terminal equipment 11, and the external storage 12, The card slot 11a provided in the information terminal equipment 11 is equipped with the end (a figure right end), And the other end (a figure lower end) is connected to the external storage 12 through the SCSI cable 14 (by a diagram, the SCSI cable 14 is drawn by bus form for simplification).
[0029]In the above system configuration, the plaintext data Xa and Xb which were developed by the main memory unit (not shown) of the information terminal equipment 11, It is enciphered by the enciphering key Ka accumulated in the predetermined region (it mentions later for details) of the computer card 13, and this is transmitted to the external storage 12 through the SCSI cable 14, and is saved as the encryption data Ya and Yb. The encryption data Ya and Yb once saved at the external storage 12, It is transmitted to the computer card 13 through the SCSI cable 14, it is decoded by the decode key Kb accumulated in the predetermined region (it mentions later for details) of this computer card 13, and the main memory unit of the information terminal equipment 11 develops.
[0030]The card I/F part 31 (I/F means an "interface".) which accomplishes the connector function at the time of equipping the card slot 11a of the information terminal equipment 11 at the end (left end of a figure) to the above-mentioned computer card 13 here as shown in drawing 2the following -- it is the same -- functional constitution of the SCSI section 32 for functional constitution being carried out, and, accomplishing the connector mechanism at the time of making connection with the SCSI cable 14 to the other end (right end of a figure) on the other hand, and performing interface converting of SCSI form between the external storages 12 of SCSI form is carried out.
[0031]The control section 33 which changes from CPU (central processing unit) etc. which control overall operation of the computer card 13 concerned to the inside of the computer card 13 on the other hand, While memorizing the cryptographic algorithm provided with the data encryption function and the data decryption function, In the plaintext data Xa developed by the basis of control of the above-mentioned control section 33, and the main memory unit of the information terminal equipment 11, and the process in which Xb is transmitted to the external storage 12. Encryption processing is sequentially performed to the plaintext data Xa concerned and Xb, using an above-mentioned cryptographic algorithm and the enciphering key Ka, The encryption data Ya and Yb which created the encryption data Ya and Yb corresponding to this, and was once written in the external storage 12 in the process transmitted to the information terminal equipment 11. Decoding processing is sequentially performed to the encryption data Ya and Yb concerned, using an above-mentioned cryptographic algorithm and the decode key Kb, Functional constitution of the encryption and the decode key accumulating part 35 which accumulates the original plaintext data Xa, the cipher-processing part 34 which restores Xb, the above-mentioned enciphering key Ka which uses the data encryption function of a cryptographic algorithm, and the above-mentioned decode key Kb which uses a data decryption function is carried out.
[0032]In addition to each above component, inside the computer card 13 concerned, While the I/F part 36 for performing necessary interface converting between the information terminal equipment 11 is formed between the above-mentioned card I/F part 31 and the control section 33, Between the above-mentioned SCSI section 32 and the control section 33, the plaintext data Xa, Xb, and the encryption data Ya and Yb which are mutually sent and received between the information terminal equipment 11 and the external storage 12 are held temporarily, and the buffer 37 for this to aim at adjustment of a data transfer rate, etc. is formed.
[0033]When the card slot 11a of the information terminal equipment 11 is equipped with the computer card 13 of the above composition as for the above-mentioned card I/F part 31, The right to access to the external storage 12 is set up automatically, and it has the function for making the information terminal equipment 11 recognize this, i.e., the function for making the information terminal equipment 11 recognize actually having been equipped with the computer card 13. If it puts in another way, it will be a function for restricting this function to the time when the card slot 11a was equipped with the computer card 13 concerned, and permitting the right to access to the external storage 12 (when it is removed, the right to

access is denied).
[0034]As mentioned above, although explained per [concerning this embodiment] example of a device, Each component 33 inside the computer card 13 mentioned above, i.e., a control section, the cipher-processing part 34, encryption and a decode key accumulating part 35, the I/F part 36, and the buffer 37, Even if it carries out functional constitution of each of that component with corresponding discrete part, it does not interfere, but it replaces with this and may be made to carry out functional constitution by the one chip element 38 which unified these each function. Since the field concerned is black-box-ized when the functional constitution by this one chip element 38 is adopted, it is very convenient when obtaining the field in which physical security is possible.
[0035]Although two kinds of keys, the enciphering key Ka and the decode key Kb, are accumulated in encryption and the decode key accumulating part 35 and the data encryption function and data decryption function of the cryptographic algorithm which were memorized by the cipher-processing part 34 were explained in the above example of a device per [which uses properly and uses two kinds of the key] technique, Besides this, accumulate the possible (the proper use at the time of using both functions is unnecessary) single common key of using both data encryption functions and data decryption functions of that cryptographic algorithm, and with this common key. Of course, it is possible to make it also make the both sides of the necessary plaintext data Xa, encryption processing of Xb, and the decoding processing of the encryption data Ya and Yb perform.
[0036]It explains per operation procedure of the example of a method applied to (the example of a method), next the example of a device explained above.
[0037]In the data encryption preserving method concerning this embodiment. As shown in drawing 3, in order to first choose the plaintext data Xa concerned and the subject equipment (in the case of this embodiment external storage 12) used as the preservation destination of Xb when saving the plaintext data Xa developed by the main memory unit of the information terminal equipment 11, and Xb, A SCSI address, i.e., the bus address in a daisy chain bus method, is chosen (ST11), and the external storage 12 concerned is changed into an accessible state.
[0038]When saving the plaintext data Xa and Xb at the external storage 12 which it changed into the accessible state here, According to write-in directions of the data from the information terminal equipment 11 (ST12), in the plaintext data Xa and the process in which Xb is transmitted to the external storage 12. The cryptographic algorithm memorized by the cipher-processing part 34 and the enciphering key Ka accumulated in encryption and the decode key accumulating part 35 are used. Encryption processing is sequentially performed to the plaintext data Xa concerned and Xb, and the encryption data Ya and Yb generated by this encryption processing corresponding to the plaintext data Xa and Xb is written in the external storage 12 (ST13).
[0039]When reading the encryption data Ya and Yb once written in the external storage 12 which it changed into the accessible state on the other hand, According to the read instruction of the data from the information terminal equipment 11 (ST12), in the process in which the encryption data Ya and Yb is transmitted to the information terminal equipment 11. The cryptographic algorithm memorized by the cipher-processing part 34 and the decode key Kb accumulated in encryption and the decode key accumulating part 35 are used, Decoding processing is sequentially performed to the encryption data Ya and Yb concerned, and the plaintext data Xa of the origin restored by this decoding processing and Xb are developed to the main memory unit of the information terminal equipment 11 (ST14).
[0040]When the enciphering key Ka and the decode key Kb were not accumulated in encryption and the decode key accumulating part 35, but it replaces with this and the single common key mentioned above is accumulated, Of course, it is made to perform the both sides of the plaintext data Xa in ST13, encryption processing of Xb, and the decoding processing of the encryption data Ya and Yb in ST14 using the common key.
[0041]According to the data encryption preserving method as for which the above result starts this embodiment, the plaintext data Xa and Xb which were developed by the main memory unit of the information terminal equipment 11, It becomes possible to save directly according to the gestalt of the encryption data Ya and Yb at the external storage 12 of SCSI form put under management of the user of a system, without once saving at the application software for document preparation. And since it is sufficient if this is not always carried but ** also carries only the small and lightweight computer card 13 when managing the external storage 12 with which the encryption data Ya and Yb was saved, the theft of the encryption data Ya and Yb by an unauthorized use person and the danger of elimination also disappear.
[0042]As mentioned above, although the embodiment of the invention was described per the example of a device, and example of a method, within limits which are not necessarily limited only to an above-

mentioned means and technique, attain the purpose said to this invention, and have an effect mentioned later, this invention can carry out change implementation suitably.

[0043]

[Effect of the Invention]As explained above, according to this invention, the plaintext data developed by the main memory unit of information terminal equipment, Without once saving at the application software for document preparation, It becomes possible to perform necessary encryption processing to the inside of a short time efficiently from the ability to save directly according to the gestalt of encryption data at external storages put under management of the user of a system, such as SCSI form.

[0044]The computer card which has a user individual's authentication function is burdened with a data encryption and function decoding, From restricting this to the time when the card slot of information terminal equipment was equipped, and having granted the right to access of the external storage to information terminal equipment. Management of the external storage with which encryption data was saved is faced, If this is not always carried but only a computer card small [**] and lightweight is removed and carried, are sufficient, As a result, it becomes possible to manage perfectly the encryption data saved at that external storage as data peculiar to a user at the same time the theft of the encryption data by the unauthorized use person of a system and the danger of elimination are eliminated.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－275115

(43)公開日　平成10年(1998)10月13日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ
			６６０Ａ
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ｚ

審査請求　未請求　請求項の数10　ＯＬ　（全 9 頁）

(21)出願番号　特願平9－80241

(22)出願日　平成９年(1997)３月31日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　河久保　秀二
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

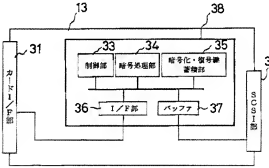
(72)発明者　高田　俊介
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　山中　喜義
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　菅　隆彦

(54)【発明の名称】　データ暗号化保存方法及びシステム装置

(57)【要約】
【課題】　外部記憶装置に保存された暗号化データを計算機カードの利用により万全に管理できるデータ暗号化保存方法及びシステム装置を提供する。
【解決手段】　制御部３３の制御のもと、情報端末装置１１の主記憶装置に展開された平文データＸａ，Ｘｂを外部記憶装置１２へ転送する過程で、暗号化・復号鍵蓄積部３５に蓄積された暗号化鍵Ｋａを用いながら当該平文データＸａ，Ｘｂに逐次的に暗号化処理を施して、対応する暗号化データＹａ，Ｙｂを作成するとともに、外部記憶装置１２に一旦書き込まれた暗号化データＹａ，Ｙｂを情報端末装置１１へ転送する過程で、暗号化・復号鍵蓄積部３５に蓄積された復号鍵Ｋｂを用いながら当該暗号化データＹａ，Ｙｂに逐次的に復号処理を施して、元の平文データＸａ，Ｘｂを復元する暗号処理部３４を、利用者個々人の認証機能を有する小型で軽量な計算機カード１３の内部に機能構成する。



1

【特許請求の範囲】

【請求項1】　情報端末装置の主記憶装置に展開された平文データの保存に際し、当該平文データの保存先を所定の環境設定に応じて外部記憶装置に設定してこれをアクセス可能な状態とし、

当該アクセス可能な状態とされた外部記憶装置に前記平文データを保存するときには、その平文データを前記外部記憶装置へ転送する過程で、所定の暗号アルゴリズム及びそのデータ暗号化機能を働かせる暗号化鍵を用いて当該平文データに逐次的に暗号化処理を施し、この暗号化処理により前記平文データに対応して生成された暗号化データを前記外部記憶装置に書き込むとともに、

当該アクセス可能な状態とされた外部記憶装置に一旦書き込まれた前記暗号化データを読み出すときには、その暗号化データを前記情報端末装置へ転送する過程で、前記所定の暗号アルゴリズム及びそのデータ復号機能を働かせる復号鍵を用いて当該暗号化データに逐次的に復号処理を施し、この復号処理により復元された元の平文データを前記情報端末装置の主記憶装置に展開する、

ことを特徴とするデータ暗号化保存方法。

【請求項2】　前記所定の暗号アルゴリズムのデータ暗号化機能を働かせる前記暗号化鍵及びデータ復号機能を働かせる前記復号鍵に代え、それぞれの機能を共に働かせる単一の共通鍵を用いて、前記平文データの暗号化処理及び前記暗号化データの復号処理を行う、

ことを特徴とする請求項1又は2記載のデータ暗号化保存方法。

【請求項3】　前記暗号化データを前記外部記憶装置へ書き込む際、及び前記外部記憶装置から前記暗号化データを読み出す際に、前記外部記憶装置のインタフェース形式に応じた所要のインタフェース変換を当該暗号化データに施す、

ことを特徴とする請求項1又は2記載のデータ暗号化保存方法。

【請求項4】　前記外部記憶装置としては、ＳＣＳＩ形式を採用したものを用い、

前記所定のインタフェース変換は、当該ＳＣＳＩ形式により行う、

ことを特徴とする請求項3記載のデータ暗号化保存方法。

【請求項5】　カード・スロットを具備した情報端末装置と、

この情報端末装置によるアクセスが可能な外部記憶装置と、

前記情報端末装置のカード・スロットに装着して使用されると共に前記外部記憶装置にケーブル接続して使用され、当該情報端末装置の主記憶装置と前記外部記憶装置との間で相互にデータ転送を行うことの可能な計算機カードと、

を有して構成され、

2

当該前記計算機カードは、

前記外部記憶装置に対するアクセス権を設定し、これを前記情報端末装置に認識させるアクセス権設定手段と、

データ暗号化機能及びデータ復号機能を備えた暗号アルゴリズムを記憶する暗号アルゴリズム記憶手段と、

この暗号アルゴリズム記憶手段に記憶された前記暗号アルゴリズムのデータ暗号化機能を働かせる暗号化鍵と、データ復号機能を働かせる復号鍵とを蓄積する鍵蓄積手段と、

前記アクセス権設定手段により当該アクセス権が設定された状態において、前記情報端末装置の主記憶装置に展開された平文データを前記外部記憶装置へ転送する過程で、前記暗号アルゴリズム記憶手段に記憶された前記暗号アルゴリズムと前記鍵蓄積手段に蓄積された前記暗号化鍵とを用いながら当該平文データに逐次的に暗号化処理を施して、前記平文データに対応する暗号化データを作成する暗号化処理手段と、

前記アクセス権設定手段により当該アクセス権が設定された状態において、前記外部記憶装置に一旦書き込まれた前記暗号化データを読み出すときに、その暗号化データを前記情報端末装置へ転送する過程で、前記暗号アルゴリズム記憶手段に記憶された前記暗号アルゴリズムと前記鍵蓄積手段に蓄積された前記復号鍵とを用いながら当該暗号化データに逐次的に復号処理を施して、元の平文データを復元する復号処理手段と、

を有する、

ことを特徴とするデータ暗号化保存システム装置。

【請求項6】　前記鍵蓄積手段は、前記暗号アルゴリズム記憶手段に記憶された前記暗号アルゴリズムのデータ暗号化機能及びデータ復号機能を共に働かせる単一の共通鍵を蓄積するものであり、

前記暗号化処理手段及び前記復号処理手段は、当該鍵蓄積手段に蓄積された前記共通鍵を用いて、それぞれ前記平文データの暗号化処理及び前記暗号化データの復号処理を行うものである、

ことを特徴とする請求項5記載のデータ暗号化保存システム装置。

【請求項7】　前記計算機カードを構成する前記暗号アルゴリズム記憶手段、前記鍵蓄積手段、前記暗号化処理手段、及び前記復号処理手段は、ワン・チップ素子により機能構成されて成る、

ことを特徴とする請求項5又は6記載のデータ暗号化保存システム装置。

【請求項8】　前記アクセス権設定手段は、前記情報端末装置のカード・スロットへの前記計算機カードの装着を以って当該アクセス権を自動的に設定し、これを前記情報端末装置に認識させるものである、

ことを特徴とする請求項5、6又は7記載のデータ暗号化保存システム装置。

【請求項９】　前記暗号化処理手段により前記暗号化データを前記外部記憶装置へ書き込む際、及び前記復号処理手段により前記外部記憶装置から前記暗号化データを読み出す際に、前記外部記憶装置のインタフェース形式に応じた所望のインタフェース変換を行うインタフェース変換手段を、

さらに有する、

ことを特徴とする請求項５、６、７又は８記載のデータ暗号化保存システム装置。

【請求項１０】　前記外部記憶装置は、ＳＣＳＩ形式を採用したものであり、

前記インタフェース変換手段は、前記所望のインタフェース変換を当該ＳＣＳＩ形式により行うものである、

ことを特徴とする請求項９記載のデータ暗号化保存システム装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データ暗号化保存方法及びシステム装置に関し、詳しくは、パーソナル・コンピュータなどの情報端末装置において作成した平文データをハード・ディスク装置などの外部記憶装置に保存する際に、その転送の過程において平文データを暗号化し、これにより外部記憶装置に保存された暗号化データを情報端末装置の主記憶装置に展開する際には、その転送の過程において暗号化データを復号するようにしたデータ暗号化保存方法、及びその実施に直接使用するデータ暗号化保存システム装置に係わる。

【０００２】【従来の技術】一般に、パーソナル・コンピュータなどの情報端末装置において作成した文書などから成る平文データを、その機密保護のために暗号化して保存しようとする場合、従来では、主記憶装置に展開された状態の作成後の平文データを、文書作成用のアプリケーション・ソフトウェアの処理に基づいて、一旦そのままの形態で内蔵ハード・ディスクなどのデータ・ファイルに保存し（即ち、文書を閉じる際の通常処理）、次いで、暗号処理用のアプリケーション・ソフトウェアの処理に基づいて、当該データ・ファイルに保存された状態の平文データに対し、所要の暗号化のための処理を実行するようにしている。

【０００３】その暗号処理用のアプリケーション・ソフトの処理につき簡単に説明すれば、図４に示すように、まず、平文データを暗号化して保存する場合には、データ・ファイル１に一旦保存されたデータを読み出して（ＳＴ１）、そのデータ形態を確認し（ＳＴ２）、それが平文データ（暗号化を行おうとしている平文データ）である場合には、所要の暗号化のための処理を実行して（ＳＴ３）、これにより得られた暗号化データをデータ・ファイル１に書き込むようにする（ＳＴ４）。

【０００４】また、以上の処理によりデータ・ファイル１に一旦保存した暗号化データを文書作成用のアプリケーション・ソフトウェア上で再び利用するには、これをデータ・ファイル１から読み出して復号した後に再びデータ・ファイル１に保存し、さらにこれを情報端末装置の主記憶装置に展開する必要があるので、上述のＳＴ２の処理において確認したデータ形態が暗号化データ（復号を行おうとしている暗号化データ）である場合には、ＳＴ３の処理において所要の復号のための処理を実行した後に、これにより得られた平文データをＳＴ４の処理においてデータ・ファイル１に書き込むようにする。

【０００５】

【発明が解決しようとする課題】以上のように、従来の平文データの暗号化処理にあっては、情報端末装置の主記憶装置に展開された当該平文データを、文書作成用のアプリケーション・ソフトウェアの処理に基づいて、必ず、データ・ファイル１に一旦保存し、その後、改めて暗号化処理を行うことが必要とされるため、その所要の暗号化処理を行うために相応の時間を要する結果となり、当該システムの利用者にとって、決して操作性が良いものとはいえない。

【０００６】また、暗号化処理により得られた暗号化データは、情報端末装置内のデータ・ファイル１に一律に保存され、そのアクセス権の管理は、通常、情報端末装置装置内のデータ管理部の属性フラグにより行われるため、この属性フラグの書き換えだけで、本来的にアクセス権のない者でも容易に当該アクセス権を変更することができる。このため、例えば、この種のシステムの構成を熟知した者に不正使用を試みられた場合などには、その不正使用者により、データ・ファイル１に保存された暗号化データが盗難されたり、或いは消去されたりする危険性がある。

【０００７】この点、例えば、暗号化データの保存先を外部ハード・ディスク装置などの外部記憶装置に設定するようにし、システムの未使用時には、その外部記憶装置を取り外すなどして、常にこれを正規の利用者の管理下におくようにすれば、上述の不正使用者による暗号化データの盗難や消去といった危険性は飛躍的に小さくなるはずである。

【０００８】しかし、外部記憶装置を常に正規の利用者の管理下におくようにするといっても、実際には極めて難しいことである。これを行うのに最も効果的なのは、システムの未使用時に、利用者が外部記憶装置を常時携帯することであるが、その大きさや重量からして実際的ではない。

【０００９】また、実際に暗号化データの管理を外部記憶装置により行う場合、そのハードウェアの変更は行わずに無改造のまま用いることが望まれる。特に、外部記憶装置の分野では、情報端末装置とのインタフェースの形式として、ＳＣＳＩ形式（ＳＣＳＩ：Small Computer System Interface）が標準化されつつあるため、でき

れば、このインタフェース形式をそのまま適用したいものである。

【0010】ここにおいて、本発明の解決すべき主要な目的は次のとおりである。即ち、本発明の第1の目的は、所要の暗号化処理を短時間のうちに効率よく行うことの可能なデータ暗号化保存方法及びシステム装置を提供することにある。

【0011】本発明の第2の目的は、所要の暗号化データの管理を外部記憶装置により行うことで、不正使用者による暗号化データの盗聴や消去などの危険性を排除するようにしたデータ暗号化保存方法及びシステム装置を提供することにある。

【0012】本発明の第3の目的は、外部記憶装置を常時携帯することなしに、その外部記憶装置に保存された暗号化データを万全に管理することの可能なデータ暗号化保存方法及びシステム装置を提供することにある。

【0013】本発明の第4の目的は、ＳＣＳＩ形式の外部記憶装置への適用が可能なデータ暗号化保存方法及びシステム装置を提供することにある。

【0014】本発明の他の目的は、明細書、図面、特に特許請求の範囲の各請求項の記載から自ずと明らかとなろう。

【0015】

【課題を解決するための手段】本発明は、上記課題の解決にあたり、情報端末装置の主記憶装置に展開された平文データから暗号化データを作成する機能を、利用者個々人の認証機能を有する計算機カード（いわゆるＰＣカード）内に構成して、この計算機カードを情報端末装置と外部記憶装置との間に介在させて用いるようにし、さらに、その計算機カードを情報端末装置に装着したときに限り、外部記憶装置のアクセス権を情報端末装置に与えるようにするという特徴を有する。

【0016】さらに、具体的詳細に述べると、当該課題の解決では、本発明が次に列挙するそれぞれの新規な特徴的構成手法及び手段を採用することにより、前記目的を達成するよう為される。

【0017】即ち、本発明方法の第1の特徴は、情報端末装置の主記憶装置に展開された平文データの保存に際し、当該平文データの保存先を所定の環境設定に応じて外部記憶装置に設定してこれをアクセス可能な状態とし、当該アクセス可能な状態とされた外部記憶装置に平文データを保存するときには、その平文データを外部記憶装置へ転送する過程で、所定の暗号アルゴリズム及びその データ暗号化機能を働かせる暗号化鍵を用いて当該平文データに逐次的に暗号化処理を施し、この暗号化処理により平文データに対応して生成された暗号化データを外部記憶装置に書き込むとともに、当該アクセス可能な状態とされた外部記憶装置に一旦書き込まれた暗号化データを読み出すときには、その暗号化データを情報端末装置へ転送する過程で、所定の暗号アルゴリズム及びそのデータ復号機能を働かせる復号鍵を用いて当該暗号化データに逐次的に復号処理を施し、この復号処理により復元された元の平文データを情報端末装置の主記憶装置に展開するデータ暗号化保存方法の構成採用にある。

【0018】本発明方法の第2の特徴は、上記本発明方法の第1の特徴における所定の暗号アルゴリズムのデータ暗号化機能を働かせる暗号化鍵及びデータ復号機能を働かせる復号鍵に代え、それぞれの機能を共に働かせる単一の共通鍵を用いて、平文データの暗号化処理及び暗号化データの復号処理を行うデータ暗号化保存方法の構成採用にある。

【0019】本発明方法の第3の特徴は、上記本発明方法の第1又は第2の特徴における暗号化データを外部記憶装置へ書き込む際、及び外部記憶装置から暗号化データを読み出す際に、外部記憶装置のインタフェース形式に応じた所要のインタフェース変換を当該暗号化データに施すデータ暗号化保存方法の構成採用にある。

【0020】本発明方法の第4の特徴は、上記本発明方法の第3の特徴における外部記憶装置として、にＳＣＳＩ形式を採用したものを用い、同特徴における所定のインタフェース変換を、当該ＳＣＳＩ形式により行うデータ暗号化保存方法の構成採用にある。

【0021】一方、本発明装置の第1の特徴は、カード・スロットを具備した情報端末装置と、この情報端末装置にアクセスが可能な外部記憶装置と、情報端末装置のカード・スロットに装着して使用されると共に外部記憶装置にケーブル接続して使用され、当該情報端末装置の主記憶装置と外部記憶装置との間で相互にデータ転送を行うことの可能な計算機カードとを有して構成され、当該計算機カードが、外部記憶装置に対するアクセス権を設定し、これを情報端末装置に認識させるアクセス権設定手段と、データ暗号化機能及びデータ復号機能を備えた暗号アルゴリズムを記憶する暗号アルゴリズム記憶手段と、この暗号アルゴリズム記憶手段に記憶された暗号アルゴリズムのデータ暗号化機能を働かせる暗号化鍵と、データ復号機能を働かせる復号鍵とを蓄積する鍵蓄積手段と、アクセス権設定手段により当該アクセス権が設定された状態において、情報端末装置の主記憶装置に展開された平文データを外部記憶装置に保存するときに、その平文データを外部記憶装置へ転送する過程で、暗号アルゴリズム記憶手段に記憶された暗号アルゴリズムと鍵蓄積手段に蓄積された暗号化鍵とを用いながら当該平文データに逐次的に暗号化処理を施して、平文データに対応する暗号化データを作成する暗号化処理手段と、アクセス権設定手段により当該アクセス権が設定された状態において、外部記憶装置に一旦書き込まれた暗号化データを読み出すときに、その暗号化データを情報端末装置へ転送する過程で、暗号アルゴリズム記憶手段に記憶された暗号アルゴリズムと鍵蓄積手段に蓄積された復号鍵とを用いながら当該暗号化データに逐次的に

復号処理を施して、元の平文データを復元する復号処理手段とを有するデータ暗号化保存システム装置の構成採用にある。

【００２２】本発明装置の第２の特徴は、上記本発明装置の第１の特徴における鍵蓄積手段が、暗号アルゴリズム記憶手段に記憶された暗号アルゴリズムのデータ暗号化機能及びデータ復号機能を共に働かせる単一の共通鍵を蓄積するものであり、同特徴における暗号化処理手段及び復号処理手段が、当該鍵蓄積手段に蓄積された共通鍵を用いて、それぞれ平文データの暗号化処理及び暗号化データの復号処理を行うものであるデータ暗号化保存システム装置の構成採用にある。

【００２３】本発明装置の第３の特徴は、上記本発明装置の第１又は第２の特徴における計算機カードを構成する暗号アルゴリズム記憶手段、鍵蓄積手段、暗号化処理手段、及び復号処理手段が、ワン・チップ素子により機能構成されて成るデータ暗号化保存システム装置の構成採用にある。

【００２４】本発明装置の第４の特徴は、上記本発明装置の第１、第２又は第３の特徴におけるアクセス権設定手段が、情報端末装置のカード・スロットへの計算機カードの装着を以って当該アクセス権を自動的に設定し、これを情報端末装置に認識させるものであるデータ暗号化保存システム装置の構成採用にある。

【００２５】本発明装置の第５の特徴は、上記本発明装置の第１、第２、第３又は第４の特徴における暗号化処理手段により暗号化データを外部記憶装置へ書き込む際、及び復号処理手段により外部記憶装置から暗号化データを読み出す際に、外部記憶装置のインタフェース形式に応じた所要のインタフェース変換を行うインタフェース変換手段をさらに有するデータ暗号化保存システム装置の構成採用にある。

【００２６】本発明装置の第６の特徴は、上記本発明装置の第５の特徴における外部記憶装置が、ＳＣＳＩ形式を採用したものであり、同特徴におけるインタフェース変換手段が、所要のインタフェース変換を当該ＳＣＳＩ形式により行うものであるデータ暗号化保存システム装置の構成採用にある。

【００２７】

【発明の実施の形態】以下、添付図面を参照しつつ、本発明の実施の形態をその装置例及び方法例につき説明する。

【００２８】（装置例）まず、本実施形態に係るデータ暗号化保存システム装置の構成は、図１に示すように、システムの基本構成として、パーソナル・コンピュータなどから成る情報端末装置１１と、この情報端末装置１１によるアクセスが可能なＳＣＳＩ形式の外部ハード・ディスク装置（通常の磁気ディスク装置や光磁気ディスク装置）などから成る外部記憶装置１２とを有して成っている。そして、本発明の主要構成部を成し、情報端末装置１１の主記憶装置と外部記憶装置１２との間で相互にデータ転送を行うことが可能な計算機カード１３は、その一端（図では右端）が、情報端末装置１１に具備されたカード・スロット１１ａに装着され、かつ、その他端（図では下端）が、ＳＣＳＩケーブル１４を通じて外部記憶装置１２に接続されるようになっている（図では、簡単化のため、ＳＣＳＩケーブル１４をバス形式で描いている）。

【００２９】以上のシステム構成において、情報端末装置１１の主記憶装置（図示せず）に展開された平文データＸａ，Ｘｂは、計算機カード１３の所定領域（詳細は後述）に蓄積された暗号化鍵Ｋａにより暗号化され、これがＳＣＳＩケーブル１４を通じて外部記憶装置１２に転送されて、暗号化データＹａ，Ｙｂとして保存されるようになっている。また、その外部記憶装置１２に一旦保存された暗号化データＹａ，Ｙｂは、ＳＣＳＩケーブル１４を通じて計算機カード１３に転送され、この計算機カード１３の所定領域（詳細は後述）に蓄積された復号鍵Ｋｂにより復号されて、情報端末装置１１の主記憶装置に展開されるようになっている。

【００３０】ここで、上述の計算機カード１３には、図２に示すように、その一端（図の左端）に、情報端末装置１１のカード・スロット１１ａに装着を行う際のコネクタ機能を成すカードＩ／Ｆ部３１（Ｉ／Ｆは「インタフェース」を意味する。以下同じ）が機能構成されており、一方、その他端（図の右端）には、ＳＣＳＩケーブル１４との接続を行う際のコネクタ機構を成し、かつ、ＳＣＳＩ形式の外部記憶装置１２との間でＳＣＳＩ形式のインタフェース変換を行うためのＳＣＳＩ部３２が機能構成されている。

【００３１】一方、計算機カード１３の内部には、当該計算機カード１３の全体的な動作を制御するＣＰＵ（中央演算処理装置）などから成る制御部３３と、データ暗号化機能及びデータ復号機能を備えた暗号アルゴリズムを記憶するとともに、上述の制御部３３の制御のもと、情報端末装置１１の主記憶装置に展開された平文データＸａ，Ｘｂを外部記憶装置１２へ転送する過程で、上述の暗号アルゴリズムと暗号化鍵Ｋａとを用いながら当該平文データＸａ，Ｘｂに逐次的に暗号化処理を施して、これに対応する暗号化データＹａ，Ｙｂを作成し、かつ、外部記憶装置１２に一旦書き込まれた暗号化データＹａ，Ｙｂを情報端末装置１１へ転送する過程で、上述の暗号アルゴリズムと復号鍵Ｋｂとを用いながら当該暗号化データＹａ，Ｙｂに逐次的に復号処理を施して、元の平文データＸａ，Ｘｂを復元する暗号処理部３４と、暗号アルゴリズムのデータ暗号化機能を働かせる前述の暗号化鍵Ｋａと、データ復号機能を働かせる前述の復号鍵Ｋｂとを蓄積する暗号化・復号鍵蓄積部３５とが機能構成されている。

【００３２】また、以上の各構成要素に加え、当該計算

機カード１３の内部には、前述のカードＩ／Ｆ部３１と制御部３３との間に、情報端末装置１１との間で所要のインタフェース変換を行うためのＩ／Ｆ部３６が設けられるとともに、前述のＳＣＳＩ部３２と制御部３３との間に、情報端末装置１１と外部記憶装置１２との間で相互に送受される平文データＸａ，Ｘｂ及び暗号化データＹａ，Ｙｂを一時的に保持し、これによりデータ転送速度の調整などを図るためのバッファ３７が設けられている。

【００３３】なお、上述のカードＩ／Ｆ部３１は、以上の構成の計算機カード１３が情報端末装置１１のカード・スロット１１ａに装着されたときに、外部記憶装置１２に対するアクセス権を自動的に設定し、これを情報端末装置１１に認識させるための機能、即ち、計算機カード１３が実際に装着されたことを情報端末装置１１に認識させるための機能も有する。換言すれば、この機能は、当該計算機カード１３がカード・スロット１１ａに装着されたときに限り、外部記憶装置１２に対するアクセス権を許容するための機能である（それが取り外されたときにはアクセス権は否定される）。

【００３４】以上、本実施形態に係る装置例につき説明したが、上述した計算機カード１３の内部の各構成要素、即ち、制御部３３、暗号処理部３４、暗号化・復号鍵蓄積部３５、Ｉ／Ｆ部３６、及びバッファ３７は、その各構成要素を対応する個別部品により機能構成しても差し支えないが、これに代え、それら各機能を統合したワン・チップ素子３８により機能構成するようにしてもよい。このワン・チップ素子３８による機能構成を採用した場合、当該領域がブラック・ボックス化されるため、物理的な機密保護が可能な領域を得る上で極めて好都合である。

【００３５】また、以上の装置例では、暗号化・復号鍵蓄積部３５に暗号化鍵Ｋａ及び復号鍵Ｋｂの２種類の鍵を蓄積しておき、暗号処理部３４に記憶された暗号アルゴリズムのデータ暗号化機能及びデータ復号機能を、その２種類の鍵を使い分けて働かせる手法につき説明したが、これ以外にも、その暗号アルゴリズムのデータ暗号化機能及びデータ復号機能を共に働かせることの可能な（双方の機能を働かせる際の使い分けが不要な）単一の共通鍵を蓄積しておき、この共通鍵によって、所要の平文データＸａ，Ｘｂの暗号化処理及び暗号化データＹａ，Ｙｂの復号処理の双方を行わせるようにすることも、勿論可能である。

【００３６】（方法例）次に、以上に説明した装置例に適用される方法例の実施手順につき説明する。

【００３７】本実施形態に係るデータ暗号化保存方法では、図３に示すように、まず、情報端末装置１１の主記憶装置に展開された平文データＸａ，Ｘｂの保存に際し、当該平文データＸａ，Ｘｂの保存先となる対象機器（本実施形態の場合、外部記憶装置１２）を選択するために、ＳＣＳＩアドレス、即ち、デイジー・チェーン・バス方式におけるバス・アドレスを選択し（ＳＴ１１）、当該外部記憶装置１２をアクセス可能な状態とする。

【００３８】ここで、アクセス可能な状態とされた外部記憶装置１２に平文データＸａ，Ｘｂを保存するときには、情報端末装置１１からのデータの書き込み指示に応じ（ＳＴ１２）、その平文データＸａ，Ｘｂを外部記憶装置１２へ転送する過程で、暗号処理部３４に記憶された暗号アルゴリズムと、暗号化・復号鍵蓄積部３５に蓄積された暗号化鍵Ｋａとを用いて、当該平文データＸａ，Ｘｂに逐次的に暗号化処理を施し、この暗号化処理により平文データＸａ，Ｘｂに対応して生成された暗号化データＹａ，Ｙｂを外部記憶装置１２に書き込む（ＳＴ１３）。

【００３９】一方、アクセス可能な状態とされた外部記憶装置１２に一旦書き込まれた暗号化データＹａ，Ｙｂを読み出すときには、情報端末装置１１からのデータの読み出し指示に応じ（ＳＴ１２）、その暗号化データＹａ，Ｙｂを情報端末装置１１へ転送する過程で、暗号処理部３４に記憶された暗号アルゴリズムと、暗号化・復号鍵蓄積部３５に蓄積された復号鍵Ｋｂとを用いて、当該暗号化データＹａ，Ｙｂに逐次的に復号処理を施し、この復号処理により復元された元の平文データＸａ，Ｘｂを情報端末装置１１の主記憶装置に展開する（ＳＴ１４）。

【００４０】なお、暗号化・復号鍵蓄積部３５に暗号化鍵Ｋａ及び復号鍵Ｋｂを蓄積せず、これに代え、前述した単一の共通鍵を蓄積しておいた場合には、無論、ＳＴ１３における平文データＸａ，Ｘｂの暗号化処理、及びＳＴ１４における暗号化データＹａ，Ｙｂの復号処理の双方を、その共通鍵を用いて行うようにする。

【００４１】以上の結果、本実施形態に係るデータ暗号化保存方法によれば、情報端末装置１１の主記憶装置に展開された平文データＸａ，Ｘｂを、文書作成用のアプリケーション・ソフトウェアに一旦保存することなしに、システムの利用者の管理下におかれたＳＣＳＩ形式の外部記憶装置１２に、暗号化データＹａ，Ｙｂの形態により直接保存することが可能となる。しかも、その暗号化データＹａ，Ｙｂの保存された外部記憶装置１２の管理に際しては、これを常時携帯せずとも、小型で軽量な計算機カード１３のみを携帯するようにすれば足りるので、不正使用者による暗号化データＹａ，Ｙｂの盗難や消去といった危険性もなくなる。

【００４２】以上、本発明の実施の形態を装置例及び方法例につき説明したが、本発明は、必ずしも上述の手段及び手法にのみ限定されるものではなく、本発明という目的を達成し、後述する効果を有する範囲内において、適宜、変更実施することが可能なものである。

【００４３】

【発明の効果】以上説明したように、本発明によれば、情報端末装置の主記憶装置に展開された平文データを、文書作成用のアプリケーション・ソフトウェアに一旦保存することなしに、システムの利用者の管理下におかれたＳＣＳＩ形式などの外部記憶装置に、暗号化データの形態により直接保存することができることから、所要の暗号化処理を短時間のうちに効率よく行うことが可能になる。

【００４４】また、利用者個々人の認証機能を有する計算機カードにデータの暗号化・復号機能を負わせ、これを情報端末装置のカード・スロットに装着したときに限り、外部記憶装置のアクセス権を情報端末装置に与えるようにしたことから、暗号化データの保存された外部記憶装置の管理に際しては、これを常時携帯せずとも、小型で軽量な計算機カードのみを取り外して携帯すれば足り、この結果、システムの不正使用者による暗号化データの盗難や消去といった危険性が排除されると同時に、その外部記憶装置に保存された暗号化データを利用者固有のデータとして万全に管理することが可能となる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るデータ暗号化保存システム装置の構成図である。

【図２】図１に示した計算機カードの内部ブロック図で＊ある。

【図３】本発明の一実施形態に係るデータ暗号化保存方法を説明するためのフロー・チャートである。

【図４】従来のデータ暗号化処理及びデータ復号処理の手法を説明するためのフロー・チャートである。

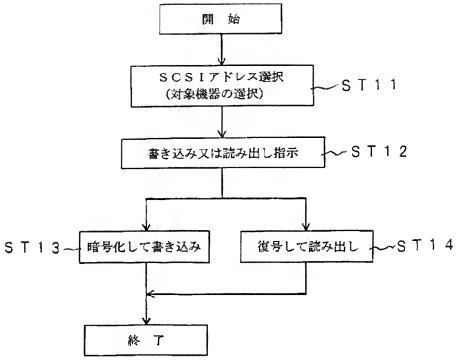
【符号の説明】

１１…情報端末装置
１１ａ…カード・スロット
１２…外部記憶装置
１３…計算機カード
１４…ＳＣＳＩケーブル
Ｘａ，Ｘｂ…平文データ
Ｙａ，Ｙｂ…暗号化データ
Ｋａ…暗号化鍵
Ｋｂ…復号鍵
３１…カードＩ／Ｆ部
３２…ＳＣＳＩ部
３３…制御部
３４…暗号処理部
３５…暗号化・復号鍵蓄積部
３６…Ｉ／Ｆ部
３７…バッファ
３８…ワン・チップ素子

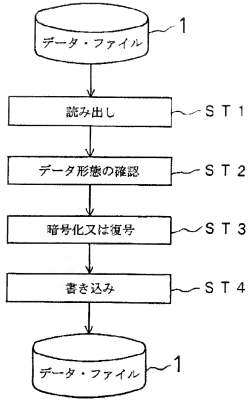
【図１】

【図２】

【図３】


開　始
ＳＣＳＩアドレス選択
（対象機器の選択）
ＳＴ１１
書き込み又は読み出し指示
ＳＴ１２
ＳＴ１３
暗号化して書き込み
復号して読み出し
ＳＴ１４
終　了

【図4】


データ・ファイル
1
読み出し
ＳＴ１
データ形態の確認
ＳＴ２
暗号化又は復号
ＳＴ３
書き込み
ＳＴ４
データ・ファイル
1